WHAT IS Claimed IS:

~~Claims~~

sub B2

1. A method of copy protecting data sent from a server to a client for presentation to a user, comprising:
cryptographically protecting the data;
sending the cryptographically protected data to the client; and
selectively controlling copying functions of the client in respect of the data whilst the data is being held by the client in a form suitable for presentation to the user.

2. A method according to claim 1 wherein the data is protected by encryption.

3. A method according to claim 1 ~~or 2~~ wherein the integrity of the data is protected cryptographically.

4. A method according to claim 3 wherein the integrity of the data is achieved by hashing.

5. A method according to claim 1 ~~any preceding claim~~ including authenticating that the client is permitted to receive the data.

6. A method according to claim 1 ~~any preceding claim~~ including identifying the client to the server before the data is sent to the client.

7. A method according to claim 1 ~~any preceding claim~~ including:
downloading a program object to the client,
running the program object on the client such that a request is uploaded to the server for a file containing the cryptographically protected data,
downloading the file to the client, and
rendering the cryptographically protected data in an unprotected form suitable

for presentation to the user,

the program object being operative such that no, or restricted, copy or save functions are offered to the user in respect of the downloaded data in its unprotected form.

8. A method according to claim 7 including downloading a message concerning a webpage wherein the message includes information concerning the program object, and uploading a request for the program object in response to said information in the message.

9. A method according to claim 8 wherein the message is in HTML code.

10. A method according to claim 8 ~~or 9~~ wherein the program object comprises a Java, Active X or OLE applet.

11. A method according to ~~any one of claims 7 to 10~~ claim 7 wherein the message is presented to the user through a browser.

12. A method according to ~~any preceding claim~~ claim 1 wherein the data is sent to the client from the server through a network.

13. A method according to claim 12 wherein the network comprises the World Wide Web.

14. A method according to ~~any one of claims 7 to 10~~ claim 7 wherein the program object includes data concerning a cryptographic key, and including using the key to render the downloaded cryptographically protected data into an unprotected form suitable for presentation to the user

15. A method according to ~~any preceding claim~~ claim 1 wherein the server and the client each hold data corresponding to a cryptographic key and a machine identifier for uniquely identifying the client, the method including:

sending a challenge to the client, such that it generates a signed response as a cryptographic function of the key and the machine identifier held therein, generating from the cryptographic key and machine identifier held associated with the server, a corresponding signed response as a cryptographic function of the key and the machine identifier,
comparing the signed responses from the client and the server, and if they correspond, performing the encryption with the key,
and performing the decryption at the client with the key.

16. A method according to ~~any preceding claim~~ Claim 1 wherein the data is steganographically marked.

17. A method according to ~~any preceding claim~~ Claim 1 including registering the client with the server.

18. A method according to ~~any preceding claim~~ Claim 1 including;
determining a machine identifier of the client by analysing its hardware and/or its software configuration,
transmitting the machine identifier to the server,
combining the transmitted machine identifier with a cryptographic key to form a unique determinator for the client,
transmitting the unique determinator to the client, to be stored therein for use subsequently in identifying the client to the server, to permit encrypted data to be downloaded thereto from the server.

19. A server configured to perform a method as claimed in ~~any preceding claim~~ Claim 1.

20. Initiation by the client, of the downloading of copy protected data by a method according to ~~any preceding claim~~ Claim 1.

21. A copy protected data stored on the client by a method according to

claim 1
~~any preceding claim.~~

22. A method of downloading encrypted data from a server to a client, including:

registering the client with the server by

determining a machine identifier of the client by analysing its hardware and/or its software configuration,

transmitting the machine identifier to the server,

combining the transmitted machine identifier with a cryptographic key to form a unique determinator for the client, and

transmitting the unique determinator to the client, to be stored therein for use subsequently in identifying the client to the server, to permit encrypted data to be downloaded thereto from the server;

subsequently identifying the client to the server on the basis of the unique determinator; and then

downloading data encrypted by means of the cryptographic key to the identified client, for decryption by the client using the key from the unique determinator.

23. A method according to claim 22 including decrypting the downloaded data at the client using the key from the unique determinator.

24. A method according to claim 22 ~~or 23~~ wherein the client is identified to the server by again determining the machine identifier for the client, comparing it with the machine identifier included in said unique determinator, and signalling to the server on the basis of the outcome of the comparison.

25. A method according to claim 22, ~~23 or 24~~ including authenticating the client to the server prior to downloading of the encrypted data.

26. A method according to claim 25 including generating a challenge, generating a response as a predetermined cryptographic function of the

cryptographic key for the client as held by the server, and as a function of the key included in the unique determinator stored in the client, and authenticating the client on the basis of the outcome of the comparison.

27. A client configured to perform a method as claimed in ~~any one of claims 22 to 26~~.